PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-004225
(43)Date of publication of application : 07.01.2000

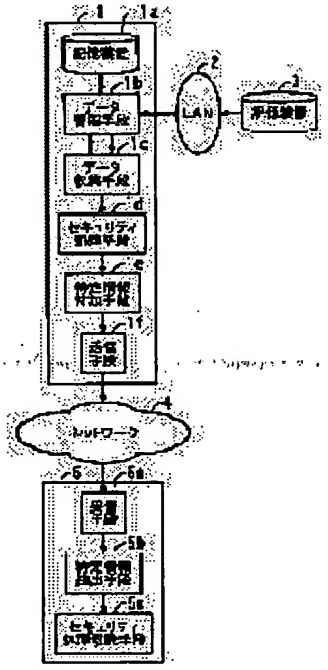
(51)Int.Cl. H04L 9/32
G06F 15/00
G09C 1/00

(21)Application number : 10-169698
(22)Date of filing : 17.06.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : TACHIBANA HIROTAKA
URITA SEIICHI
KOTANI MASATAKE
HAYASHI TAKEHIKO

(54) NETWORK SYSTEM, TRANSMISSION/RECEPTION METHOD, TRANSMITTER, RECEIVER AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To safely transmit data to a called party independently of the skill of an end user or the like.
SOLUTION: A data managing means 1b of a transmitter 1 unitarily manages data stored in a storage device 1a or 3. When the transmission of data is requested from terminal equipment not shown in Figure connected to the transmitter 1, a data collecting means 1c collects the desired data while referring to the data managing means 1b. A security processing means 1d performs security processing corresponding to the secrecy level of collected data. A specified information adding means 1e adds specified information for specifying the security processing to data. A transmission means 1f transmits data, to which security processing is performed, through a network 4 to a receiver 5. A reception means 5a of the receiver 5 receives data from the transmitter 1. A specified information extracting means 5b extracts the specified information added to the data. While referring to the specified information, a security processing releasing means 5c releases security processing applied to the data.



LEGAL STATUS

[Date of request for examination] 29.07.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－4225
（P2000－4225A）
(43)公開日　平成12年１月７日(2000.1.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
H04L 9/32		H04L 9/00	671	5B085
G06F 15/00	330	G06F 15/00	330A	5K013
G09C 1/00	660	G09C 1/00	660E	

審査請求　未請求　請求項の数14　ＯＬ　（全 24 頁）

(21)出願番号　特願平10－169698

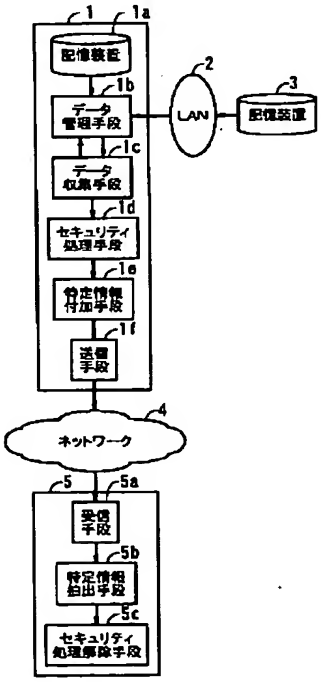
(22)出願日　平成10年６月17日(1998.6.17)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　橋　博隆
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　瓜田　誠一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100092152
弁理士　服部　毅巖

最終頁に続く

(54)【発明の名称】　ネットワークシステム、送受信方法、送信装置、受信装置、および、記録媒体

(57)【要約】
【課題】　セキュリティ処理を統合化する
【解決手段】　送信装置１のデータ管理手段１ｂは、記憶装置１ａまたは記憶装置３に記憶されているデータを一元的に管理する。データ収集手段１ｃは、送信装置１に接続されている図示せぬ端末装置からデータの送信要求がなされた場合には、データ管理手段１ｂを参照して所望のデータを収集する。セキュリティ処理手段１ｄは、収集されたデータの秘匿レベルに応じたセキュリティ処理を施す。特定情報付加手段１ｅは、セキュリティ処理を特定するための特定情報をデータに付加する。送信手段１ｆは、ネットワーク４を介して受信装置５にセキュリティ処理が施されたデータを送信する。受信装置５の受信手段５ａは送信装置１からのデータを受信する。特定情報抽出手段５ｂは、データに付加されている特定情報を抽出する。セキュリティ処理解除手段５ｃは、特定情報を参照してデータに施されているセキュリティ処理を解除する。



1

【特許請求の範囲】

【請求項１】　送信装置において、データにセキュリティ処理を施した後、受信装置に送信するネットワークシステムにおいて、

送信装置は、

送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段と、

前記セキュリティ処理手段によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段と、

前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信する送信手段と、を有し、

受信装置は、

前記ネットワークを介して伝送されてきたデータを受信する受信手段と、

前記データに付加されている前記特定情報を抽出する特定情報抽出手段と、

前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段と、を有することを特徴とするネットワークシステム。

【請求項２】　前記送信装置は、記憶装置に格納されているデータを一元管理するデータ管理手段と、

前記データ管理手段を参照して、送信しようとするデータを収集するデータ収集手段と、

を更に有することを特徴とする請求項１記載のネットワークシステム。

【請求項３】　前記セキュリティ処理手段は、受信側のアクセス権限レベルも加味してセキュリティ処理を行うことを特徴とする請求項１記載のネットワークシステム。

【請求項４】　前記セキュリティ処理手段は、前記受信装置とネットワークとからなるシステムのシステム安全レベルも加味してセキュリティ処理を行うことを特徴とする請求項３記載のネットワークシステム。

【請求項５】　前記送信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、送信側のアクセス権限レベルおよびシステム安全レベルを与える第１のテーブルと、得られたこれら３つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第２のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第２のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して、施されたセキュリティ要素処理とその処理順序とを示す情報を特定情報として付加し、

2

前記特定情報抽出手段は、セキュリティ要素処理とその処理順序とを示す情報を受信したデータから抽出し、

前記セキュリティ処理解除手段は、抽出されたセキュリティ要素処理の組み合わせとその処理順序とを示す情報を参照して、セキュリティ処理を解除することを特徴とする請求項４記載のネットワークシステム。

【請求項６】　新たなセキュリティ要素処理を追加するセキュリティ要素処理追加手段を更に有することを特徴とする請求項５記載のネットワークシステム。

【請求項７】　既存のセキュリティ要素処理を更新するセキュリティ要素処理更新手段を更に有することを特徴とする請求項５記載のネットワークシステム。

【請求項８】　前記送信装置および受信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、送信側のアクセス権限レベルおよびシステム安全レベルを与える第１のテーブルと、得られたこれら３つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第２のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第２のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、

前記特定情報抽出手段は、受信したデータから前記送信元名とデータ名とを抽出し、

前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせと処理順序を前記第１および第２のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項４記載のネットワークシステム。

【請求項９】　前記送信装置および受信装置の双方がアクセスできるネットワーク上の所定の位置に、送信しようとするデータのデータ秘匿レベル、ならびに、送信側のアクセス権限レベルおよびシステム安全レベルを与える第１のテーブルと、得られたこれら３つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第２のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第２のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、

前記特定情報抽出手段は、前記送信元名とデータ名とを

受信したデータから抽出し、
前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせとその処理順序とを前記第１および第２のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項４記載のネットワークシステム。
【請求項１０】　送信装置において、データにセキュリティ処理を施した後、受信装置に送信する送受信方法において、
送信装置は、
送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施し、
施されたセキュリティ処理を特定するための特定情報を前記データに対して付加し、
前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信し、
受信装置は、
前記ネットワークを介して伝送されてきたデータを受信し、
前記データに付加されている前記特定情報を抽出し、
前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する、
ことを特徴とする送受信方法。
【請求項１１】　データにセキュリティ処理を施した後、受信装置に対して送信する送信装置において、
送信しようとするデータにデータ属性、送受環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段と、
前記セキュリティ処理手段によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段と、
前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信する送信手段と、
を有することを特徴とする送信装置。
【請求項１２】　データにセキュリティ処理を施した後、受信装置に対して送信する送信処理をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体において、
コンピュータを、
送信しようとするデータにデータ属性、送受環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段、
前記セキュリティ処理手段によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段、
前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信する送信手段、
として機能させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１３】　送信装置においてセキュリティ処理が施されたデータを受信する受信装置において、
ネットワークを介して前記送信装置から伝送されてきたデータを受信する受信手段と、
前記データに付加されている特定情報を抽出する特定情報抽出手段と、
前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段と、
を有することを特徴とする受信装置。
【請求項１４】　送信装置においてセキュリティ処理が施されたデータを受信する受信処理をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体において、
コンピュータを、
ネットワークを介して前記送信装置から伝送されてきたデータを受信する受信手段、
前記データに付加されている特定情報を抽出する特定情報抽出手段、
前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段、
として機能させるプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はネットワークシステム、送受信方法、送信装置、受信装置、および、記録媒体に関し、特に、送信装置においてデータにセキュリティ処理を施した後、受信装置に送信するネットワークシステムとその送受信方法、セキュリティ処理を施したデータを送信する送信装置、送信装置でセキュリティ処理が施されたデータを受信する受信装置、セキュリティ処理を施したデータを送信する送信処理をコンピュータに実行させるプログラムを記録した記録媒体、および、送信装置でセキュリティ処理が施されたデータを受信する受信処理をコンピュータに実行させるプログラムを記録した記録媒体に関する。
【０００２】
【従来の技術】ネットワークを介してデータを送る場合には、データの漏洩や改竄などを未然に防ぐため、種々のセキュリティ処理（例えば、暗号化処理など）を施したデータを送信する場合が多い。
【０００３】
【発明が解決しようとする課題】ところで、ある企業から他の企業に対してデータを送信するような場合には、以下のような手順を踏む必要があった。
（１）送信側の企業の社内ＬＡＮなどに分散して格納されている所望のデータを収集する。

（２）個々のデータの秘匿レベルを、例えば、社内規約などを参照して調べる。

（３）得られたデータの秘匿レベルに加え、送信時に利用するネットワーク種（専用回線、ＶＡＮ（Value Added Network）、または、オープンネットワークなど）や送信先のシステム環境などを総合的に考慮して、適用すべきセキュリティ処理を決定する。

（４）個々のデータに対して、決定されたセキュリティ処理を逐次適用する。

（５）セキュリティ処理の内容を受信側に対して通知する。

（６）セキュリティ処理を施したデータを受信側に対して送信する。

【０００４】従って、各プロセスにおいて、以下のような問題点があった。（１）に関しては、所望のデータが格納されている場所を検索し、その場所から手作業でデータを取得する必要があるので、作業が非効率的であるという問題点があった。また、データを物理的にコピーする（ある記録媒体から他の記録媒体にコピーする）ので、同一コンテンツのデータが複数存在することになる。そのため、データの更新時のタイムラグなどによりデータの正当性が保証できない（版数が異なる可能性がある）という問題点があった。（２）に関しては、エンドユーザが個別にデータの秘匿レベルを調査するので、作業が非効率的であり、また、社内規約などを参照して秘匿レベルを主観的に判定することから、セキュリティ処理レベルの統一が困難であるという問題点があった。更に、秘匿レベルの社内規約などが変更された場合には、その通達に時間を要することから、最悪の場合には重要情報が外部に漏れる可能性があるという問題点があった。（３）に関しては、複数のデータを送信する場合に、作業の煩雑性から、個々のデータ毎にきめ細かくセキュリティ処理を設定することが困難であるという問題点があった。そのため、一般的に秘匿レベルの一番高いデータに合わせてセキュリティ処理を施すことが多いので、処理が非効率的になる（重要ではないデータに対してもレベルの高いセキュリティ処理を施すことになる）。また、社内規約書だけでは対応しきれないケースに関しては、エンドユーザのスキルに依存することになり、セキュリティ処理の平準化が困難であるという問題点もあった。更に、相手企業との規約が変更されたような場合、新規処理への移行に時間を要するという問題点もあった。（４）に関しては、エンドユーザが必要なセキュリティ処理用のソフトウエアを購入し、セットアップし、また、運用する必要があるため、作業負荷が大きいという問題点があった。また、セキュリティ処理用のソフトウエアはエンドユーザの端末に導入されていることが通例であるため、例えば、ソフトウエアのバージョンアップがなされた場合には、受信側との間でバージョンの不整合が生じ、セキュリティ処理が施されたデータを復号できなくなるといった不都合が生じることもあった。更に、新たなソフトウエアが追加されたような場合にも同様の不都合が生じる。更にまた、エンドユーザがセキュリティ処理の処理手順を誤った場合には、処理の効果が著しく減少したり（例えば、暗号化したデータを圧縮しても十分に圧縮できない）、処理自体が無意味になる（例えば、暗号化したデータにウィルス処理を施しても効果は期待できない）。また、エンドユーザがセキュリティ処理を忘れてしまったような場合には、重要な情報が社外に漏洩することになるという問題点もあった。（５）に関しては、例えば、送信されてきたデータを復号するための手続きを忘れてしまったような場合には、データを復号することが不可能になるという問題点があった。また、受信側では、各社毎（または担当者毎）に異なるセキュリティ処理に対応する必要があるため、作業の負担が大きいという問題点もあった。

【０００５】本発明はこのような点に鑑みてなされたものであり、エンドユーザの習熟度などに依存することなく、データを安全に送信先に伝送することを可能とするネットワークシステムおよび送受信方法を提供することを目的とする。

【０００６】また、本発明は、送信しようとするデータに対してセキュリティ処理を施す場合に、エンドユーザの負担を軽減することを可能とする送信装置を提供することを目的とする。

【０００７】更に、送信側で施されたセキュリティ処理を人手を介さずに確実に復号することを可能とする受信装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明では上記課題を解決するために、図１に示ように、送信装置１においてデータにセキュリティ処理を施した後、受信装置５に送信するネットワークシステムにおいて、送信装置１は、送信しようとするデータのデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を前記データに施すセキュリティ処理手段１ｄと、前記セキュリティ処理手段１ｄによって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段１ｅと、前記特定情報が付加されたデータをネットワーク４を介して所定の受信装置に対して送信する送信手段１ｆと、を有し、受信装置５は、前記ネットワーク４を介して伝送されてきたデータを受信する受信手段５ａと、前記データに付加されている前記特定情報を抽出する特定情報抽出手段５ｂと、前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段５ｃと、を有することを特徴とするネットワークシステムが提供される。

【０００９】ここで、送信装置１のセキュリティ処理手段１ｄは、送信しようとするデータにデータ属性、送受

信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施す。特定情報付加手段１ｅは、セキュリティ処理手段１ｄによって施された処理を特定するための特定情報をデータに対して付加する。送信手段１ｆは、特定情報が付加されたデータをネットワーク４を介して所定の受信装置に対して送信する。受信装置５の受信手段５ａは、ネットワーク４を介して伝送されてきたデータを受信する。特定情報抽出手段５ｂは、データに付加されている特定情報を抽出する。セキュリティ処理解除手段５ｃは、特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する。

【００１０】また、データにセキュリティ処理を施した後、受信装置５に対して送信する送信装置１において、送信しようとするデータにデータ属性、送受信環境から特定される秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段１ｄと、前記セキュリティ処理手段１ｄによって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段１ｅと、前記特定情報が付加されたデータをネットワーク４を介して所定の受信装置に対して送信する送信手段１ｆと、を有することを特徴とする送信装置が提供される。

【００１１】ここで、セキュリティ処理手段１ｄは、送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施す。特定情報付加手段１ｅは、セキュリティ処理手段１ｄによって施された処理を特定するための特定情報をデータに対して付加する。送信手段１ｆは、特定情報が付加されたデータをネットワーク４を介して所定の受信装置に対して送信する。

【００１２】更に、送信装置１においてセキュリティ処理が施されたデータを受信する受信装置５において、ネットワーク４を介して前記送信装置１から伝送されてきたデータを受信する受信手段５ａと、前記データに付加されている特定情報を抽出する特定情報抽出手段５ｂと、前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段５ｃと、を有することを特徴とする受信装置が提供される。

【００１３】ここで、受信手段５は、ネットワーク４を介して送信装置１から伝送されてきたデータを受信する。特定情報抽出手段５ｂは、データに付加されている特定情報を抽出する。セキュリティ処理解除手段５ｃは、特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は、本発明の原理を説明する原理図である。この図において、送信装置１は、記憶装置１ａ、データ管理手段１ｂ、データ収集手段１ｃ、セキュリティ処理手段１ｄ、特定情報付加手段１ｅ、および、送信手段１ｆによって構成されている。また、送信装置１は、ＬＡＮ２を介して記憶装置３と接続されている。

【００１５】受信装置５は、ネットワーク４を介して送信装置１と接続されている。受信装置５は、受信手段５ａ、特定情報抽出手段５ｂ、および、セキュリティ処理解除手段５ｃによって構成されている。

【００１６】送信装置１の記憶装置１ａは、例えば、ＨＤＤ（Hard Disk Drive ）などによって構成されており、種々のデータ（送信の対象となるデータ）を記憶している。

【００１７】データ管理手段１ｂは、記憶装置１ａおよび記憶装置３に記憶されているデータを、例えば、論理データベースなどにより一元管理する。データ収集手段１ｃは、送信しようとするデータをデータ管理手段１ｂの論理データベースを参照して収集する。

【００１８】セキュリティ処理手段１ｄは、データ収集手段１ｃによって収集されたデータに対して、そのデータ秘匿レベルに対応するセキュリティ処理を施す。特定情報付加手段１ｅは、セキュリティ処理手段１ｄによって施されたセキュリティ処理を特定するための特定情報をデータに対して付加する。

【００１９】送信手段１ｆは、特定情報が付加されたデータをネットワーク４を介して受信装置５に向けて送信する。受信装置５の受信手段５ａは、ネットワーク４を介して伝送されてきたデータを受信する。

【００２０】特定情報抽出手段５ｂは、データに付加されている特定情報を抽出する。セキュリティ処理解除手段５ｃは、特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する。

【００２１】次に、以上の原理図の動作について説明する。いま、送信装置１に接続されている端末装置（図示せず）から、記憶装置１ａおよび記憶装置３に格納されている所定の情報（例えば、パーソナルコンピュータの設計情報）を送信する要求がなされたとすると、データ収集手段１ｃは、関連するデータ（例えば、マザーボードの設計情報、ハードディスクドライブの設計情報、および、グラフィックカードの設計情報など）を取得する要求をデータ管理手段１ｂに対して行う。

【００２２】データ管理手段１ｂは、例えば、記憶装置１ａおよび記憶装置３に格納されているデータを論理的に階層化して管理している（例えば、パーソナルコンピュータの設計情報を、ツリー型の階層構造により系統的に管理している）論理データベース（以下、ＤＢと適宜略記する）を格納しており、データ収集手段１ｃは、この論理ＤＢを参照して所望のデータを記憶装置１ａまたは記憶装置３から取得してセキュリティ処理手段１ｄに供給する。

【００２３】セキュリティ処理手段１ｄは、データ収集手段１ｃより供給されたデータに付加されているデータ

秘匿レベルを抽出する。即ち、記憶装置１ａおよび記憶装置３に記憶されているデータには、それぞれのデータの重要度を示すデータ秘匿レベル（その値が高いほど重要な情報であることを示す）が付加されており、セキュリティ処理手段１ｄは、データ収集手段１ｃより供給されたデータに付加されているデータ秘匿レベルを抽出する。

【００２４】そして、セキュリティ処理手段１ｄは、抽出したデータ秘匿レベルに対応するセキュリティ処理を個々のデータに対して施す。例えば、データ秘匿レベルが低い場合には、圧縮処理のみを施し、秘匿レベルが高くなるにつれて、暗号化処理や認証処理などを適切な順序で組み合わせて施す。即ち、圧縮処理は暗号化処理の前に施さなければデータの圧縮率が低下するので、これら双方の処理を施す場合には、圧縮処理、暗号化処理の順序で行う。なお、以下では、セキュリティ処理を構成する個々のセキュリティ処理（例えば、暗号化処理、認証処理、および、圧縮処理など）を「セキュリティ要素処理」と適宜記述する。

【００２５】特定情報付加手段１ｅは、セキュリティ処理が施されたデータに対して、施されたセキュリティ要素処理の種類とその処理順序を特定するための特定情報を付加する。

【００２６】送信手段１ｆは、特定情報が付加されたデータをネットワーク４を介して受信装置４に向けて送信する。受信装置５の受信手段５ａは、ネットワーク４を介して送信装置１から伝送されてきたデータを受信し、特定情報抽出手段５ｂに供給する。

【００２７】特定情報抽出手段５ｂは、受信手段５ａから供給されたデータから特定情報を抽出し、データとともにセキュリティ処理解除手段５ｃに供給する。セキュリティ処理解除手段５ｃは、特定情報抽出手段５ｂから供給された特定情報を参照して、送信装置１において施されたセキュリティ要素処理の種類とその処理順序とを認知し、その逆の順序でセキュリティ要素処理をデータに対して施す。その結果、データを復号することができる。例えば、圧縮処理と暗号化処理が施されている場合には、暗号の復号処理を施した後、伸長処理を施すことによりもとのデータを得る。

【００２８】このようにして復号されたデータは、図示せぬ記憶装置などに格納され、受信装置５側のエンドユーザの要求に応じて、表示装置などに表示出力することが可能となる。

【００２９】なお、以上の説明では、送信しようとする個々のデータに対して、個別のセキュリティ処理を施すようにしたが、送信しようとするデータのうち、最も高い秘匿レベルを有するデータに合わせて全てのデータにセキュリティ処理を施すようにしてもよい。

【００３０】以上に述べたように、本発明では、送信装置１側のエンドユーザが所望の情報を送信しようとした場合には、先ず、データ収集手段１ｃが、データ管理手段１ｂに記憶されている論理ＤＢを参照して所望の情報に関連するデータを自動的に収集する。次に、セキュリティ処理手段１ｄが、収集されたデータに付加されているデータ秘匿レベルに応じて、所定のセキュリティ要素処理を適切な順序で組み合わせてデータに施す。そして、セキュリティ処理が施されたデータは、施されたセキュリティ要素処理の種類とその処理順序を特定するための特定情報が付加されて受信装置５に向けて送信される。

【００３１】続いて、受信装置５では、受信手段５ａが送信装置１から伝送されてきたデータを受信する。特定情報抽出手段５ｂは、受信したデータから特定情報を抽出し、セキュリティ処理解除手段５ｃが特定情報を参照してデータに施されているセキュリティ処理を解除する。

【００３２】従って、本発明によれば、送信側のエンドユーザが手作業で必要なデータを収集する必要がなくなるため、作業の効率を向上させることができるとともに、データの正当性が保証される。

【００３３】また、送信側のエンドユーザの個別の判断によらず、データの秘匿レベルに応じて自動的にセキュリティ処理が施されるので、セキュリティ処理レベルを平準化することが可能となるとともに、不注意によって重要な情報が外部に漏洩することを防止することができる。

【００３４】更に、社内規約などの規約書だけでは判定が困難なデータに対しても的確なセキュリティ処理がなされるので、エンドユーザのスキルに依存しないセキュリティシステムを構築することができる。

【００３５】更にまた、セキュリティ要素処理が統合的に管理されているため、例えば、あるセキュリティ要素処理がバージョンアップされた場合は、送信装置１に格納されている要素処理のみを変更するだけでよいので、個々のエンドユーザにかかる負担を軽減することができる。

【００３６】また、常に最適な順序でセキュリティ要素処理が施されることから、個々の要素処理の効果を最大限に発揮させることが可能となる。更に、特定情報を参照して処理が自動的に実行されることから、処理手続きを別途送信する手間を省略することができるとともに、処理手順を喪失したことによって、データの復号が不可能となることを防止することができる。

【００３７】次に、図２および図３を参照して、本発明の実施の形態の構成例について説明する。図２は、本発明の送信装置の実施の形態の構成例を示すブロック図である。この図において、送信装置１０は、端末装置２２～２４などから入力された各種のデータを統合的に管理するとともに、端末装置２２～２４などから所定の情報に対する送信要求がなされた場合には、対応する情報を

取得してネットワーク３０を介して後述する受信装置に向けて送信する。

【００３８】表示装置１９は、例えば、ＣＲＴ（Cathode Ray Tube）モニタによって構成されており、送信装置１０から出力される画像信号を表示出力する。ＬＡＮ（Local Area Network）２０は、例えば、イーサネット（Ethernet）などであり、サーバ２１および端末装置２２～２４を相互に接続し、これらの間でデータの授受を可能とする。

【００３９】サーバ２１は、種々のデータを記憶した記憶装置を具備しており、端末装置２２～２４または送信装置１０の要求に応じてデータを検索し、ＬＡＮ２０を介して要求を行った装置に対して送信する。また、端末装置２２～２４から所定のデータが入力された場合には、送信装置１０を経由して、記憶装置の所定の領域に格納する。

【００４０】端末装置２２～２４は、各エンドユーザが使用するものであり、所望の情報を受信装置に対して送信したり、新たなデータをサーバ２１に登録する。ネットワーク３０は、例えば、専用回線、ＶＡＮ、または、オープンネットワーク（例えば、インターネット）などによって構成されている。

【００４１】次に、送信装置１０の詳細な構成について説明する。送信装置１０は、ＣＰＵ（Central Processing Unit）１１、ＲＯＭ（Read Only Memory）１２、ＲＡＭ（Random Access Memory）１３、ドライバ１４、ＨＤＤ１５、ＩＦ（Interface）１６，１７、および、バス１８によって構成されている。

【００４２】ＣＰＵ１１は、装置の各部を制御するとともに種々の演算処理を実行する。ＲＯＭ１２は、ＣＰＵ１１が実行する基本的なプログラム（ファームウエア）や各種データなどを記憶している。ＲＡＭ１３は、ＣＰＵ１１が各種演算処理を実行する場合に、演算途中のデータやプログラムなどを一時的に格納する。

【００４３】ドライバ１４は、ＣＰＵ１１から供給される描画命令に応じた描画処理を行い、得られた画像を画像信号に変換して表示装置１９に出力する。ＨＤＤ１５は、論理データベース１５ａ、データ秘匿レベルテーブル１５ｂ、アクセス権限レベルテーブル１５ｃ、システム安全レベルテーブル１５ｄ、セキュリティ設定多次元テーブル１５ｅ、および、セキュリティフィルタ管理テーブル１５ｆを有している。また、セキュリティ要素処理を行うソフトウエアなども格納している。

【００４４】論理データベース１５ａは、サーバ２１およびその他の記憶装置（例えば、端末装置２２～２４に具備されている記憶装置など）に記憶されているデータを、論理的に階層付けて管理している。

【００４５】例えば、パーソナルコンピュータのマザーボードに関する情報が図４に示す構造を有しているとする。即ち、マザーボードＢ－Ｍ－０１は、Ｆ社製のコンポーネントＢ－Ｓ－０１と、他社製のコンポーネントＢ－Ｓ－０２から構成されている。また、コンポーネントＢ－Ｓ－０１は、ＣＰＵ（Ｂ－Ｃ－００）と電源Ｂ－Ｃ－１０とによって構成されている。更に、コンポーネントＢ－Ｓ－０２は、メモリＢ－Ｃ－２０とコネクタＢ－Ｃ－３０とによって構成されている。

【００４６】このような構造を有するパーソナルコンピュータのマザーボードの設計情報を、例えば、サーバ２１および他の記憶装置に分散して格納した場合の格納の一態様を図５に示す。この例では、コンポーネントＢ－Ｓ－０１に関する情報が、記憶装置６０（例えば、サーバ２１の図示せぬ記憶装置）に格納され、コンポーネントＢ－Ｓ－０２に関するデータが、記憶装置６１，６２（例えば、端末装置２２，２３）に分散されて格納されている。また、図４では示していないが、ＣＰＵ（Ｂ－Ｃ－００）、電源Ｂ－Ｃ－１０、メモリＢ－Ｃ－２０、および、コネクタＢ－Ｃ－３０は、それぞれコンポーネントＢ－Ｃ－０１とＢ－Ｃ－０２、Ｂ－Ｃ－１１とＢ－Ｃ－１２、Ｂ－Ｃ－２１とＢ－Ｃ－２２、および、Ｂ－Ｃ－３１とＢ－Ｃ－３２によって構成されている。

【００４７】なお、各データの末尾のハッチングを施した部分は、各データの属性情報を示しており、例えば、記録日時、更新日時、および、データサイズなどの情報である。

【００４８】図６は、論理データベース１５ａに格納されている情報であり、図５に示すデータの階層構造を示している。この図において、各四角形内に示されている文字列（例えば、Ｂ－Ｍ－０１）は、データ名を示しており、記憶装置に格納する場合のファイル名である。また、ハッチングが施されている部分は、属性情報であり、そのデータが格納されている記憶装置やその位置に関する情報が格納されている。

【００４９】このように、論理データベース１５ａは、物理的に分散して格納されている個々のデータの対応関係に関する情報を保有しており、このような情報を参照することにより、上位の階層にある所定の情報を指定した場合にはそれに関連する（階層がそれよりも下の）情報を特定するとともに、その格納場所を簡単に取得することが可能となる。例えば、送信する情報として、「Ｂ－Ｃ－１０」を指定した場合には、「Ｂ－Ｃ－１１」と「Ｂ－Ｃ－１２」がその下位の情報であり、また、属性情報によりそれらの格納場所を特定することができる。

【００５０】図２に戻って、データ秘匿レベルテーブル１５ｂは、図７に示すように、記憶装置に記憶されているデータの秘匿レベルを格納している。図７に示す例では、ＰＣ（パーソナルコンピュータ）に関する情報は、マザーボード、ＨＤＤ、および、その他の情報から構成されており、更にマザーボードに関する情報は、設計書、コスト、および、生産計画から構成されている。この例では、マザーボードの設計書の秘匿レベルは、

“６”であり、コストおよび生産計画に関する情報は、それぞれ“１０”および“５”である。この秘匿レベルが高いほど重要な情報であることを示す。

【００５１】なお、サーバ２１などにデータを格納する場合には、その重要度に応じたデータ秘匿レベルをデータ秘匿レベルテーブル１５ｂに登録する。このような作業は、各セクションの担当者や送信装置１０の管理者が一括して行うようにすれば、各データ間の秘匿レベルを平準化することができる。

【００５２】図２に戻って、アクセス権限レベルテーブル１５ｃは、図８に示すように送信相手のアクセス権限レベルを格納している。図８の例では、送信相手の企業に対して、部門およびその業務内容に応じてアクセス権限レベルが割り当てられている。

【００５３】例えば、Ｆ社のＡ部門は、そのＩＤが“０１”であり、業務として「ＰＣ」を担当しているセクションのアクセス権限レベルは、“１”である。また、ＨＤＤを担当しているセクションのアクセス権限レベルは、“３”である。なお、このアクセス権限レベルが高いほど、重要な情報をアクセスできることを示している。

【００５４】図２に戻って、システム安全レベルテーブル１５ｄは、図９に示すように送信相手のシステムの安全レベルを格納している。図９の例では、送信相手の企業がその部門別に安全レベルを付与されている。なお、「ネット環境」は、ネットワークに対する安全レベルの評価であり、例えば、専用線であるかインターネットであるかによって安全レベルが査定される。「システム環境」は、使用されるコンピュータシステムに対する安全レベルの評価であり、汎用機、ＵＮＩＸ機、パーソナルコンピュータなどに応じて査定される。「運用環境」は、専用オペレータがいるか、または、ルールが明確であるかなどに応じて査定される。「総合環境」は、ネット環境、システム環境、および、運用環境の平均値であり、この値がシステム安全レベルとして利用される。例えば、Ｆ社のＡ部門は、ネット環境は“６”であり、また、システム環境および運用環境はそれぞれ“７”，“５”である。その結果、これらの平均値である総合環境は、“６”（＝（６＋７＋５）／３）となる。なお、この総合環境の値が大きいほど、システムの総合的な安全レベルが高いことを示している。

【００５５】なお、平均値ではなく、各環境の査定値に所定の重み係数を乗算し、得られた結果を加算して得られる値を用いるようにしてもよい。そのような構成によれば、各環境の安全レベルが与える影響を正確に反映した値を求めることが可能となる。

【００５６】図２に戻って、セキュリティ設定多次元テーブル１５ｅは、図１０に示すように、データ秘匿レベルα、アクセス権限レベルβ、および、システム安全レベルγをパラメータとして対応するフィルタを特定する。ここで、フィルタとは複数のセキュリティ要素処理を最適な順序で組み合わせたものを指している。このセキュリティ設定多次元テーブル１５ｅの原理について以下に説明する。

【００５７】いま、α，β，γを軸とする直交座標系を考える。データ秘匿レベルαはその値が大きくなるほど重要な情報であることから、αの値が原点から離れるに従ってレベルの高いセキュリティ処理を施す必要が生じる。

【００５８】また、アクセス権限レベルβは、その値が大きくなるほど、重要な情報をアクセス可能であることから、値が大きいほど信頼性の高い送信相手である。従って、βの値は原点に近いほどレベルの高いセキュリティ処理を施す必要がある。

【００５９】更に、システム安全レベルγは、その値が大きくなるほど送信相手のシステムの信頼性が高いことから、γの値が原点に近づくほどレベルの高いセキュリティ処理を施す必要がある。従って、α，β，γ座標系における位置に応じて、データに施すべきセキュリティ処理（フィルタ）を決定するようにすれば、そのデータに最適なセキュリティ処理を選択することが可能となる。

【００６０】図１０に示すセキュリティ設定多次元テーブル１５ｅでは、α，β，γ座標系の定義域を８つの互いに独立な領域（互いに重なり合わない領域）に分割し、それぞれの領域と、その領域に最適なセキュリティ処理を示すフィルタＮｏ．とを対応付けている。

【００６１】例えば、データ秘匿レベルαが範囲（１≦α＜５）内にあり、アクセス権限レベルβが範囲（２＜β≦６）内にあり、また、システム安全レベルが範囲（２＜β≦６）内にある場合には、表の第１番目の項目であるＮｏ．１のフィルタが選択されることになる。

【００６２】なお、α，β，γの定義域は、１≦α，β，γ≦１０であるが、図１０に示すセキュリティ設定多次元テーブル１５ｅでは、α≧９、β≦２、および、γ≦２が除外されている。これは、α，β，γの何れかがこのような範囲にある場合には、十分なセキュリティが確保できないことから、データの送信を行わないようにするためである。従って、α，β，γの何れかがこのような範囲にある場合には、データの送信処理が直ちに停止される。

【００６３】図２に戻って、セキュリティフィルタ管理テーブル１５ｆは、図１１に示すように、各フィルタＮｏ．に対応するセキュリティ要素処理の種類とその処理順序とを管理している。ここで、記号ａ～ｆは、図１２に示すように、各セキュリティ要素処理の分類（例えば、認証処理、署名処理、・・・）を示しており、また、ａ～ｆを更に細分する数字はその処理の処理内容（例えば、分類ｅに関しては、ＬＨＡ、ＣＯＭＰＲＥＳＳ、・・・）を示している。

【００６４】次に、本発明の受信装置の実施の形態の構成例について説明する。図３は、本発明の受信装置の構成例を示すブロック図である。なお、この図において図２に示す送信装置と対応する部分には、対応する符号を付してあるのでその説明は省略する。

【００６５】受信装置４０は、送信装置１０とほぼ同様の構成とされているが、ＨＤＤ４５に格納されているテーブルの種類が異なっている。即ち、送信装置１０のＨＤＤ１５に格納されているテーブルから、データ秘匿レベルテーブル１５ｂ、アクセス権限レベルテーブル１５ｃ、システム安全レベルテーブル１５ｄ、セキュリティ設定多次元テーブル１５ｅ、および、セキュリティフィルタ管理テーブル１５ｆが除外され、セキュリティ規約テーブル４５ｇが付加されている。

【００６６】セキュリティ規約テーブル４５ｇは、送信装置１０から送信されたデータに付加されているフィルタＮｏ．を参照して、対応するセキュリティ要素処理とその処理順序とを与えるように構成されている。

【００６７】その他の構成は、図２に示す送信装置１０と同様であるのでその説明は省略する。次に、図１３を参照して図２に示す実施の形態の動作について説明する。

【００６８】図１３は、図２に示す実施の形態がデータを送信する場合に実行する処理の一例を説明するフローチャートである。このフローチャートが開始されると、以下の処理が実行される。

［Ｓ１］ＣＰＵ１１は、ドライバ１４に対して所定の描画指令を供給し、図１４に示す送信画面を表示装置１９に表示させる。

【００６９】図１４は、この処理の結果、表示装置１９に表示される送信画面の一例である。この表示例では、「送信画面」と題されたダイアログボックス７０に、送信元設定領域７１、送信先設定領域７２、および、送信データ設定領域７３が表示されている。また、ダイアログボックス７０の右上部には、このダイアログボックスのサイズを変更したり設定を終了するためのボタン７７～７９が表示されている。更に、ダイアログボックス７０の右下部には、設定した内容でデータを送信する場合に操作される送信ボタン８０と設定内容をキャンセルする場合に操作されるＣＡＮＣＥＬボタン８１とが具備されている。

【００７０】送信元設定領域７１には、コンボボックス７１ａ～７１ｄが表示されており、それぞれ、送信者名、送信者の所属する部門、その部門のＩＤ、および、その部門の業務内容が入力される。

【００７１】送信先設定領域７２には、コンボボックス７２ａ～７２ｃが表示されており、それぞれ、受信者名、受信者の所属する部門、その部門のＩＤが入力される。送信データ設定領域７３には、リストボックス７３ａとエディットボックス７３ｂが表示されている。リストボックス７３ａには送信するデータの候補がツリー形式で表示される。なお、この表示は、論理データベース１５ａを参照して行われる。リストボックス７３ａの右側には、垂直スクロールバー７４～７６が表示されており、所望のデータを検索する場合に操作される。

【００７２】リストボックス７３ａにおいて送信対象となるデータを選択すると、選択された内容は送信されるデータとしてエディットボックス７３ｂに表示される。

［Ｓ２］ＣＰＵ１１は、図１４に示す送信画面において全ての必要項目の入力が終了し、送信ボタン８０が操作され場合にはステップＳ３に進み、それ以外の場合にはステップＳ２に戻る。

［Ｓ３］ＣＰＵ１１は、図１４に示す送信画面において入力された送信先に関する情報を取得する。

【００７３】図１４の例では、受信者として「Ｇ社」が入力されており、その部門とＩＤとして「Ａ部門」および「０１」が入力されているので、これらの情報が取得されることになる。

［Ｓ４］ＣＰＵ１１は、図１４に示す送信画面において入力された送信データ名を取得する。

【００７４】図１４の例では、エディットボックス７３ｂに表示されている「マザーボード設計書」が送信データ名として取得されることになる。

［Ｓ５］ＣＰＵ１１は、ステップＳ４において取得した送信データ名に対応するデータを論理データベース１５ａを参照して、サーバ２１または他の記憶装置から収集する。

【００７５】図１４の例では、図５に示すように複数の記憶装置に分散して格納されているマザーボード設計書に関するデータが収集されることになる。

［Ｓ６］ＣＰＵ１１は、データ秘匿レベルテーブル１５ｂを参照して、収集したデータの秘匿レベルを取得する。

【００７６】いま、図１４に示す送信画面において入力されたマザーボードの設計情報は、図７に示すようにその秘匿レベルが、“６”であることから、ＣＰＵ１１は秘匿レベルとして“６”を取得することになる。

［Ｓ７］ＣＰＵ１１は、アクセス権限レベルテーブル１５ｃを参照して、送信先のアクセス権限レベルを取得する。

【００７７】いま、図１４に示す送信画面において入力された送信先（Ｇ社のＡ部門）は、図８に示すようにそのアクセス権限レベルが、“２．１”であることから、ＣＰＵ１１はアクセス権限レベルとして“２．１”を取得することになる。

［Ｓ８］ＣＰＵ１１は、システム安全レベルテーブル１５ｄを参照して、送信先のシステム安全レベルを取得する。

【００７８】いま、図１４に示す送信画面において入力された送信先（Ｇ社のＡ部門）は、図９に示すようにそ

のシステム安全レベル（総合環境）が、“２．１”であることから、ＣＰＵ１１はシステム安全レベルとして“２．１”を取得することになる。

［Ｓ９］ＣＰＵ１１は、ステップＳ６～８において取得したデータ秘匿レベルα、アクセス権限レベルβ、および、システム安全レベルγに対応するフィルタＮｏ．を取得する。

【００７９】いま、データ秘匿レベルα＝６、アクセス権限レベルβ＝２．１、および、システム安全レベルγ＝２．１であることから、これをα，β，γ座標系上に★印としてプロットすると図１５のようになる。

【００８０】この★印は、図１０に示すセキュリティ設定多次元テーブルの第５番目に記載されている範囲（５≦α＜９，２＜β≦６，２＜γ≦６）に含まれている。従って、図１４の入力例では、対応するフィルタＮｏ．として“５”が取得されることになる。

［Ｓ１０］ＣＰＵ１１は、ステップＳ５において収集したデータに対して、ステップＳ１０において取得したフィルタＮｏ．のセキュリティ処理を施す。

【００８１】いま、ステップＳ９の処理においてフィルタＮｏ．５が取得されたことから、ＣＰＵ１１は、図１１に示すセキュリティフィルタ管理テーブル１５ｆを参照してフィルタＮｏ．５に対応するセキュリティ要素処理を特定する。この例では、対応するセキュリティ要素処理として、ａ－１、ｂ－２、ｅ－１、および、ｆ－１が特定される。具体的には、これらの処理は、図１２に示すように、「ＰＣ－ＣＡＲＤ」、「ＭＤ５」、「ＬＨＡ」、および、「ＤＥＳ」処理である。

【００８２】従って、ＣＰＵ１１は、これらの処理を指定された順序でＨＤＤ１５から読み出し、ステップＳ５において収集したデータに施す。この処理の概要を示したのが図１７である。Ｎｏ．５のフィルタでは、機能ａ，ｂ，ｅ，ｆが選択されているので、これらの機能が“オン”の状態とされ、それ以外の機能ｃ，ｄはオフの状態とされている。送信しようとするデータは、図の左から右へ進むうちに、セキュリティ要素処理ａ－１、ｂ－２、ｅ－１、ｆ－１が施される。なお、これらのセキュリティ要素処理は、前述のように最適な順序で配置されているので、効率よくデータにセキュリティ処理を施すことができる。

［Ｓ１１］ＣＰＵ１１は、セキュリティ処理が施されたデータをＩＦ１７に供給し、そこで、データをパケット化させる。

【００８３】図１８は、パケット化されたデータの一例を示している。この例では、セキュリティ処理されたデータ９６の先頭に、ヘッダ９０、送信元９１、送信先９２、データ名９３、送信日時９４、および、フィルタＮｏ．９５が付加されている。

【００８４】ヘッダ９０は、通信プロトコルの種類やデータの種類を特定するための情報を含んでいる。送信元９１および送信先９２は、送信元と送信先の名称などの情報を含んでいる。データ名９３は、セキュリティ処理されたデータ９６のデータ名を含んでいる。送信日時９４は、このパケットを送信した日時を含んでいる。フィルタＮｏ．９５は、データに施されたセキュリティ処理のフィルタＮｏ．を含んでいる。

［Ｓ１２］ＩＦ１７は、パケット化したデータをネットワーク３０を介して送信先の受信装置４０に向けて送信する。

【００８５】ところで、以上では、送信しようとするデータの全てが同一の秘匿レベルである場合について述べたが、例えば、一部の秘匿レベルが異なるデータを送信する場合について以下に説明する。

【００８６】いま、図５に示す、複数の記憶装置に分散して記憶されているデータのうち、電源Ｂ－Ｃ－１０の秘匿レベルが“６”から“１”に変更されたとする。図１９に秘匿レベルが変更されたデータの一例を示す。この例では、記憶装置６０に記憶されているデータの一部（図中２重線で囲繞されている部分）の秘匿レベルが変更されている。また、図２０は、階層構造を示す図上において、秘匿レベルが変更されたデータ（図中２重線で囲繞した部分）の位置を示している。

【００８７】図２１は、図７に示すデータ秘匿レベルテーブル１５ｂが、電源の秘匿レベルの変更に伴って改訂された場合の一例を示す。この例では、図７の場合と比較して、資料名「設計書」が更に細分化されており、そのうちの電源の秘匿レベルのみが“１”に設定されている。

【００８８】このようなデータに対してセキュリティ処理を施す場合、「ＣＰＵ」、「メモリ」、および、「コネクタ」の秘匿レベルは不変であるので、これらに対しては、前述の場合と同様のセキュリティ処理が施される。

【００８９】しかし、「電源」に対しては、その秘匿レベルが“６”から“１”に変更されていることから、α，β，γの値はそれぞれ（１，２．１，２．１）となり、α，β，γ座標系における位置は図２２に示す★印のようになる。

【００９０】この★印は、図２３に示すように、フィルタＮｏ．１に対応する範囲（１≦α＜５，２＜β≦６，２＜γ≦６）に含まれていることから、図１３のステップＳ９では、フィルタＮｏ．として“１”が取得される。

【００９１】従って、ステップＳ１０では、「ＣＰＵ」、「メモリ」、および、「コネクタ」に対応するデータに対しては、前述の場合と同様にＮｏ．５のフィルタによってセキュリティ処理が施される。一方、「電源」に対応するデータに対しては、Ｎｏ．１のフィルタによってセキュリティ処理が施される。即ち、Ｎｏ．１のフィルタは、図１１に示すようにセキュリティ処理機

能ａ，ｄよりなり、また、その処理内容は図１２に示すように、認証処理である「ＰＣ－ＣＡＲＤ」とウィルス処理である「ＶＡＣＣＩＮＥ」から構成されるので、図２４に示すような手順により、セキュリティ処理が施されることになる。

【００９２】即ち、図２４に示すように、セキュリティ要素処理ａ，ｄのみがオンの状態とされ、その他は全てオフの状態とされているので、図の左側から入力されたデータは、セキュリティ処理機能ａに対応する「ＰＣ－ＣＡＲＤ」とセキュリティ処理機能ｄに対応する「ＶＡＣＣＩＮＥ」とが施されることになる。

【００９３】そして、以上のようにしてセキュリティ処理が施されたデータは、ＩＦ１７に供給されてそこでパケット化される。このとき、「電源」に対応するデータに対しては、フィルタＮｏ．９５（図１８参照）として“１”が格納され、一方、その他のデータに対しては、“５”が格納されて送信されることになる。

【００９４】従って、秘匿レベルが異なるデータをまとめて送信する場合には、それぞれのデータに最適なセキュリティ処理が施されて送信されることになる。また、社内規約の変更などに伴って、所定のデータの秘匿レベルが変更されたような場合には、データ秘匿レベルテーブル１５ｂの内容を変更するだけで、そのデータに施されるセキュリティ処理を即座に変更することができるので、ここのエンドユーザにかかる負担を軽減することが可能となるとともに、重要な情報が社外に漏洩することを防止することができる。

【００９５】次に、以上のようにして送信されたデータが受信装置４０によって受信される場合の処理について説明する。図２５は、図３に示す受信装置４０がデータを受信する場合に実行する処理の一例を示すフローチャートである。このフローチャートが開始されると、以下の処理が実行されることになる。

［Ｓ２１］ＩＦ４７は、ネットワーク３０を介して送信装置１０から伝送されてきたパケットを受信し、ＲＡＭ４３またはＨＤＤ４５に逐次格納する。

［Ｓ２２］ＣＰＵ４１は、受信処理が終了したか否かを判定し、終了した場合にはステップＳ２３に進み、それ以外の場合にはステップＳ２２に戻る。

［Ｓ２３］ＣＰＵ４１は、受信したパケットからフィルタＮｏ．を取得する。

［Ｓ２４］ＣＰＵ４１は、受信したパケットからデータを取得する。

［Ｓ２５］ＣＰＵ４１は、セキュリティ規約テーブル４５ｇを参照して、ステップＳ２３で取得したフィルタＮｏ．に対応するセキュリティ要素処理をデータに対して順次施し、データに施されているセキュリティ処理を解除する。

【００９６】即ち、セキュリティ規約テーブル４５ｇには、図１１および図１２に示すような情報が格納されているので、ＣＰＵ４１は、このテーブルに記載されている情報を参照して、ステップＳ２３において抽出したフィルタＮｏ．に対応するセキュリティ要素処理の種類とその処理順序を取得する。

【００９７】そして、取得した処理順序の逆の順番でセキュリティ要素処理をデータに対して施すことによりもとのデータを得る。例えば、フィルタＮｏ．が“５”である場合には、ＣＰＵ４１は、受信したデータに対して「ＤＥＳ」、「ＬＨＡ」、「ＭＤ５」、および、「ＰＣ－ＣＡＲＤ」をこの順序で施すことになる。

【００９８】このようにしてセキュリティ処理が解除されたデータは、ＨＤＤ４５などに一旦格納された後、表示装置４９などに表示して閲覧することが可能となる。

次に、送信装置１０のセキュリティ設定多次元テーブル１５ｅの設定内容を変更する場合の処理について説明する。

【００９９】図２６は、図２に示す送信装置１０のセキュリティ設定多次元テーブル１５ｅの設定内容を変更する場合に表示される設定画面の表示例である。この表示例では、「設定画面」と題されたダイアログボックス１００が表示されている。ダイアログボックス１００の右上には、このボックスの表示サイズを変更したり、処理を終了する場合に操作されるボタン１０１～１０３が表示されている。

【０１００】また、ボックス内の最上部には、設定対象フィルタＮｏ．設定部１０４が表示されており、コンボボックスの右端に表示されている矢印ボタンを操作することにより表示されるプルダウンメニューの中から所望の項目を選択することで、設定の対象とするフィルタのＮｏ．を選択することができる。この例では、値“４”が選択されていることから、フィルタＮｏ．４が設定の対象となる。

【０１０１】データ秘匿レベルα設定部１０５では、αの範囲が入力される。この例では、αの下限と上限とに対応するコンボボックスが表示されており、これらのコンボボックスを操作することにより所望の値を選択することが可能となる。この例では、“５”および“９”が選択されている。

【０１０２】また、アクセス権限レベルβ設定部１０６には、βの範囲が入力される。更に、システム安全レベルγ設定部１０７には、γの値が入力される。また、記号「≦」の部分を１回押圧すると、記号「＜」が表示される。また、再度押圧すると記号「≦」が再表示される。従って、この部分を適宜押圧することにより所望の記号を選択することができる。

【０１０３】なお、このようにして入力された範囲が、他のフィルタの範囲と重なっている場合には、設定内容が意味を持たなくなるため、警告を出したり、その値が入力できなくなるようにしてもよい。

【０１０４】このようにして入力された設定値を、セキ

ュリティ設定多次元テーブル１５ｅに登録する場合には登録ボタン１０８を操作する。その結果、ＣＰＵ１１は、設定画面上において入力された設定値を、ＨＤＤ１５のセキュリティ設定多次元テーブル１５ｅの所定の領域に書き込むことになる。

【０１０５】なお、ＣＡＮＣＥＬボタン１０９が操作されると、入力された設定値がキャンセルされ、もとのデータ（変更前のデータ）がセキュリティ設定多次元テーブル１５ｅから読み出されて表示される。

【０１０６】更に、削除ボタン１１０が操作されると、ＨＤＤ１５のセキュリティ設定多次元テーブル１５ｅに既に登録されているデータのうち、設定対象フィルタＮｏ．によって指定されるデータが削除されることになる。

【０１０７】以上の処理によれば、セキュリティ設定多次元テーブル１５ｅの設定値を目的に応じて適宜設定することが可能となる。次に、送信装置１０のセキュリティフィルタ管理テーブル１５ｆの設定内容を変更する場合の処理について説明する。

【０１０８】図２７は、図２に示す送信装置１０のセキュリティフィルタ管理テーブル１５ｆの設定内容を変更する場合に表示される設定画面の表示例である。この表示例では、「設定画面」と題されたダイアログボックス１２０が表示されている。ダイアログボックス１２０の右上には、このボックスの表示サイズを変更したり、処理を終了する場合に操作されるボタン１２１～１２３が表示されている。

【０１０９】ダイアログボックス１２０は、「フィルタ設定画面」と題されたフィルタ設定領域１２４と「登録／削除画面」と題されたフィルタ登録／削除領域１２５とから構成されている。

【０１１０】フィルタ設定領域１２４においては、セキュリティフィルタ管理テーブル１５ｆの設定内容が設定内容表示領域１２４ａに表示される。所定の設定項目を変更する場合には、設定内容表示領域１２４ａの右端に設けられている垂直スクロールバー１２６または矢印ボタン１２７，１２８、および、下端に設けられている水平スクロールバー１２９または矢印ボタン１３０，１３１を適宜操作して所望の領域を表示させた後、所望の数値を入力または削除することにより、設定内容を変更することができる。

【０１１１】また、登録／削除領域１２５においては、各セキュリティ要素処理の処理内容の設定を行うことができる。「分類」と表示されたコンボボックス１２５ａには、セキュリティ要素処理の分類（例えば、認証、署名、圧縮など）が入力される。

【０１１２】「枝番」と表示されたコンボボックス１２５ｂには、セキュリティ要素処理の枝番号（例えば、１，２，・・・）が入力される。なお、この枝番は、図１２に示す「Ｎｏ．」に対応している。

【０１１３】「処理内容」と表示されたコンボボックス１２５ｃには、セキュリティ要素処理の内容（例えば、ＰＣ－ＣＡＲＤ、ＭＤ５、Ｗ－ＭＡＲＫなど）が入力される。また、その下のコンボボックス１２５ｄには、処理内容に関する付記事項などが入力される。

【０１１４】「運用開始」と表示されたコンボボックス１２５ｅには、セキュリティ要素処理の運用が開始される日時（例えば、１９９９年８月１０日　午前１０時）が入力される。

【０１１５】「有効期限」と表示されたコンボボックス１２５ｆには、セキュリティ要素処理の運用期限の日時（例えば、２００１年８月１０日　午前１０時）が入力される。

【０１１６】また、「登録者」と表示されたコンボボックス１２５ｇには、セキュリティ要素処理の登録を行った登録者の氏名（例えば、「橘　博隆」など）が入力される。

【０１１７】このような設定画面において登録された内容を登録する場合には、登録ボタン１３２を操作する。この登録ボタン１３２が操作されると、ＣＰＵ１１は、設定画面において入力された情報を取得し、ＨＤＤ１５のセキュリティフィルタ管理テーブル１５ｆの所定の領域に書き込む。その結果、図２７に示す設定画面において入力された情報が登録されることになる。

【０１１８】また、入力した情報を登録せずにキャンセルする場合には、ＣＡＮＣＥＬボタン１３３を操作する。すると、ＣＰＵ１１は、入力された情報を消去するとともに、ＨＤＤ１５のセキュリティフィルタ管理テーブル１５ｆから変更前の情報を読み出してダイアログボックス１２０の所定の位置に表示する。その結果、登録処理を最初から行うことが可能となる。

【０１１９】更に、登録／削除領域１２５に表示されている処理内容を削除する場合には、削除ボタン１３４を操作する。この削除ボタン１３４が操作されると、ＣＰＵ１１は、登録／削除領域１２５に表示されている処理内容に対応する処理を、ＨＤＤ１５から削除する。その結果、不要な処理をＨＤＤ１５から削除することが可能となる。

【０１２０】なお、コンボボックス１２５ｅ，１２５ｆから入力された運用開始日時と有効期限とを参照して、対応するセキュリティ要素処理を自動的に運用開始または運用停止するようにしてもよい。

【０１２１】即ち、ＣＰＵ１１は、セキュリティフィルタ管理テーブル１５ｆに登録されているセキュリティ要素処理を実行する場合に、この運用開始日時と有効期限とを参照して、運用期限内である場合にのみ対応する要素処理をデータに対して施すようにすればよい。このような構成によれば、セキュリティ要素処理を運用期間に応じて自動的に管理することが可能となる。

【０１２２】以上に述べたように、本発明によれば、送

信しようとするデータの秘匿レベルのみならず、送信相手のアクセス権限レベルおよびシステム安全レベルも参照してセキュリティ処理を決定するので、総合的な条件に基づいたセキュリティ処理を施すことができる。

【０１２３】また、セキュリティ要素処理を変更したりバージョンアップする場合などにおいても、送信装置１０に登録されているデータを変更するだけで事足りることから、エンドユーザにかかる負担を軽減することができる。

【０１２４】更に、各記憶装置に格納されているデータは、論理データベース１５ａによって一元管理されているため、必要なデータを集めたり版数を管理する手間を省くことが可能となる。

【０１２５】なお、以上の実施の形態においては、個々のデータの秘匿レベルをデータ秘匿レベルテーブル１５ｂに格納するようにしたが、例えば、それぞれのデータに秘匿レベルを付加して記憶装置に記憶するようにしてもよい。

【０１２６】そのような構成によれば、同一のデータが複数のエンドユーザによって利用された場合においても、セキュリティ処理を均一化することが可能となる。

次に、図２８を参照して、本発明のネットワークシステムの第２の実施の形態について説明する。

【０１２７】図２８は、本発明のネットワークシステムの第２の実施の形態の受信装置の構成例を示すブロック図である。なお、この図において、図３と対応する部分には同一の符号を付してあるので、その説明は省略する。また、第２の実施の形態の送信装置は、図２の場合と同様の構成とされているのでその説明は省略する。

【０１２８】この実施の形態では、図３の場合と比較してＨＤＤ４５に格納されているテーブルが異なっている。即ち、図２８に示す実施の形態では、セキュリティ規約テーブル４５ｇが除外され、データ秘匿レベルテーブル４５ｂ、アクセス権限レベルテーブル４５ｃ、システム安全レベルテーブル４５ｄ、セキュリティ設定多次元テーブル４５ｅ、および、セキュリティフィルタ管理テーブル４５ｆが新たに追加されている。なお、このＨＤＤ４５に記憶されているテーブルは、図２に示す送信装置１０に記憶されているものと同様の構成とされている。

【０１２９】次に、第２の実施の形態の動作について説明する。いま、図２に示す送信装置１０の端末装置２２～２４の何れかにより所定のデータの送信要求がなされたとすると、第１の実施の形態と同様の処理が行われ、データにセキュリティ処理が施されることになる。

【０１３０】セキュリティ処理が施されたデータは、ＩＦ１７に供給され、そこでパケット化されることになる。第２の実施の形態においては、図２９に示すように、図１８に示す第１の実施の形態のパケットから、フィルタＮｏ．９５が除外されたパケットが送信される。

【０１３１】このようなパケットを受信した受信装置４０は、先ず、パケットに含まれている送信元９１、送信先９２、および、データ名９３を取得する。前述のように、受信装置４０のＨＤＤ４５に格納されているテーブルは、送信装置１０のＨＤＤ１５に記憶されているものと同様であることから、抽出したデータ名９３からデータ秘匿レベルを特定し、また、送信元９１および送信先９２からアクセス権限レベルとシステム安全レベルとを特定する。

【０１３２】そして、特定されたこれらのレベルをセキュリティ設定多次元テーブル４５ｅおよびセキュリティフィルタ管理テーブル４５ｆに適用することにより、送信側で施されたセキュリティ処理を特定することができる。

【０１３３】ＣＰＵ４１は、前述のようにして特定されたフィルタＮｏ．のセキュリティ要素処理を、送信側とは逆の順序によりデータに施す。その結果、送信側で施されたセキュリティ処理を解除してもとのデータを得ることができる。

【０１３４】以上の構成によれば、送信側から受信側に対してフィルタＮｏ．を送信する必要がなくなることから、送信するデータのデータ量を削減することが可能となる。

【０１３５】次に、図３０および図３１を参照して、本発明の第３の実施の形態の構成例について説明する。なお、これらの図において、図２および図３と対応する部分には同一の符号を付してあるのでその説明は省略する。

【０１３６】図３０は、本発明の第３の実施の形態の送信装置の構成例を示すブロック図である。この実施の形態においては、図２の場合と比較して、論理データベース１５ａ以外の全てのテーブルがＨＤＤ１５から除外されている。また、ネットワーク３０にサーバ１４０およびＨＤＤ１４１が新たに追加されている。その他の構成は、図２の場合と同様である。

【０１３７】また、図３１は、本発明の第３の実施の形態の受信装置の構成例を示すブロック図である。この実施の形態においては、図３の場合と比較して、ＨＤＤ４５に格納されているセキュリティ規約テーブル４５ｇが除外されている。また、図３０の場合と同様に、ネットワーク３０にサーバ１４０およびＨＤＤ１４１が新たに追加されている。その他の構成は、図３の場合と同様である。

【０１３８】サーバ１４０は、送信装置１０または受信装置４０からの要求に応じてＨＤＤ１４１に記憶されているデータをネットワーク３０を介して送信する。ＨＤＤ１４１は、セキュリティ処理に関するテーブルを格納している。即ち、ＨＤＤ１４１は、図３２に示すように、データ秘匿レベルテーブル１４１ｂ、アクセス権限レベルテーブル１４１ｃ、システム安全レベルテーブル

１４１ｄ、セキュリティ設定多次元テーブル１４１ｅ、および、セキュリティフィルタ管理テーブル１４１ｆを格納している。なお、これらのテーブルは、図２に示すＨＤＤ１５に格納されているものと同様であるのでその説明は省略する。

【０１３９】次に、以上の実施の形態の動作について説明する。いま、図３０に示す、端末装置２２～２４の何れかにより、所定のデータの送信要求がなされたとすると、ＣＰＵ１１は、ＨＤＤ１５に格納されている論理データベース１５ａを参照して、対応するデータを記憶装置から取得する。

【０１４０】そして、ＣＰＵ１１は、ネットワーク３０を介してサーバ１４０から、収集したデータの秘匿レベル、送信先のアクセス権限レベル、および、システム安全レベルとを取得するとともに、これらの値に応じたセキュリティ要素処理とその処理順序を取得する。そして、取得した処理順序に従って、セキュリティ要素処理をデータに施し、ＩＦ１７に供給する。

【０１４１】ＩＦ１７は、セキュリティ処理が施されたデータを図２９に示すようなパケットにパケット化して受信装置４０に向けて送信する。このようなパケットを受信した受信装置４０のＣＰＵ４１は、パケットから送信元９１、送信先９２、および、データ名９３を抽出し、これらに対応するセキュリティ処理のフィルタＮｏ．をサーバ１４０から取得する。

【０１４２】そして、ＣＰＵ４１は、取得したフィルタＮｏ．に対応するセキュリティ要素処理を逆の順序で、セキュリティ処理されたデータ９６に対して施すことにより元のデータを得る。

【０１４３】以上の実施の形態によれば、送信側と受信側のテーブルが共有化されることから、ネットワーク全体のセキュリティ処理の統合化を図ることが可能となる。なお、上記の処理機能は、コンピュータによって実現することができる。その場合、送信装置および受信装置が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述されており、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリなどがある。

【０１４４】市場に流通させる場合には、ＣＤ－ＲＯＭ(Compact Disk Read Only Memory)やフロッピーディスクなどの可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置などにプログラムを格納しておき、メインメモリにロードして実行するようにすればよい。

【０１４５】

【発明の効果】以上説明したように本発明によれば、送信装置では、送信データにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応したセキュリティ処理を施すとともに、施されたセキュリティ処理を特定する特定情報を付加して送信し、受信装置では、特定情報を参照してセキュリティ処理を解除するようにしたので、複数のエンドユーザによってデータが送信されるような場合においても、平準化されたセキュリティ処理を施すことが可能となる。

【０１４６】また、エンドユーザの負担を増大させることなく、確実なセキュリティ処理を施すことが可能となる。

【図面の簡単な説明】

【図１】本発明の原理を説明する原理図である。

【図２】本発明の送信装置の第１の実施の形態の構成例を示すブロック図である。

【図３】本発明の受信装置の第１の実施の形態の構成例を示すブロック図である。

【図４】図２に示す実施の形態に格納されているデータの一例を示す図である。

【図５】図２に示す記憶装置に格納されているデータの格納の一態様を示す図である。

【図６】図２に示す論理データベースに格納されている情報の一例を示す図である。

【図７】図２に示すデータ秘匿レベルテーブルに格納されている情報の一例を示す図である。

【図８】図２に示すアクセス権限レベルテーブルに格納されている情報の一例を示す図である。

【図９】図２に示すシステム安全レベルテーブルに格納されている情報の一例を示す図である。

【図１０】図２に示すセキュリティ設定多次元テーブルに格納されている情報の一例を示す図である。

【図１１】図２に示すセキュリティフィルタ管理テーブルに格納されている情報の一例を示す図である。

【図１２】図２に示すセキュリティフィルタ管理テーブルに格納されている他の情報の一例を示す図である。

【図１３】図２に示す実施の形態がデータを送信する場合に実行する処理の一例を説明するフローチャートである。

【図１４】図１３に示すフローチャートが実行された場合に、表示装置に表示される送信画面の表示例である。

【図１５】図２に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図１６】図２に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図１７】図２に示す実施の形態において実行されるセキュリティ処理の原理を説明する図である。

【図１８】図２に示す実施の形態から送信されるデータの構造の一例を示す図である。

【図１９】図５に示すデータの一部が変更された場合を

示す図である。

【図２０】図１９に示すデータの論理構造を示す図である。

【図２１】図１９に示すデータに対応するデータ秘匿レベルテーブルを示す図である。

【図２２】図２に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図２３】図２に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図２４】図２に示す実施の形態において実行されるセキュリティ処理の原理を説明する図である。

【図２５】図３に示す実施の形態がデータを受信する場合に実行する処理の一例を説明するフローチャートである。

【図２６】図２に示すセキュリティ設定多次元テーブルを設定する場合に表示される設定画面の表示例である。

【図２７】図２に示すセキュリティフィルタ管理テーブルを設定する場合に表示される設定画面の表示例である。

【図２８】本発明の受信装置の第２の実施の形態の構成例を示すブロック図である。

【図２９】図２８に示す実施の形態が受信するデータの構造を示す図である。

【図３０】本発明の送信装置の第３の実施の形態の構成例を示すブロック図である。

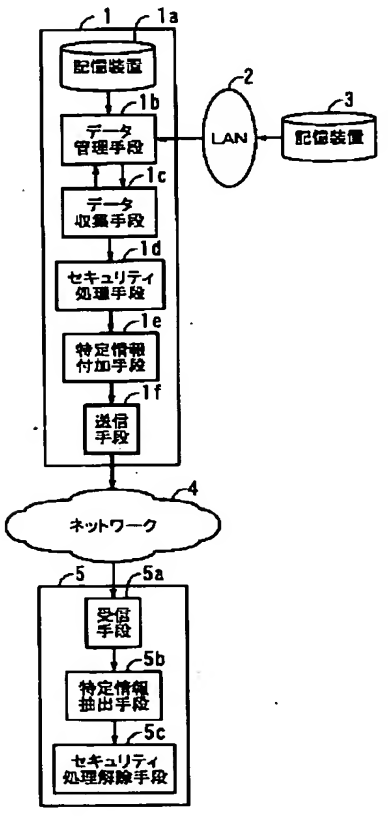
【図３１】本発明の受信装置の第３の実施の形態の構成例を示すブロック図である。

【図３２】図３０に示す実施の形態のサーバに付随するＨＤＤに格納されているデータの一例を示す図である。

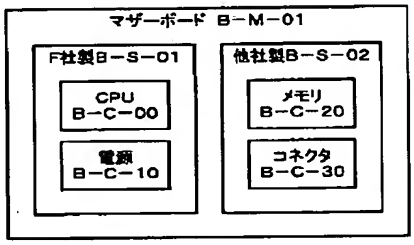
【符号の説明】

1　送信装置
1a　記憶装置
1b　データ管理手段
1c　データ収集手段
1d　セキュリティ処理手段
1e　特定情報付加手段
1f　送信手段
2　ＬＡＮ
3　記憶装置
4　ネットワーク
5　受信装置
5a　受信手段
5b　特定情報抽出手段
5c　セキュリティ処理解除手段

【図１】



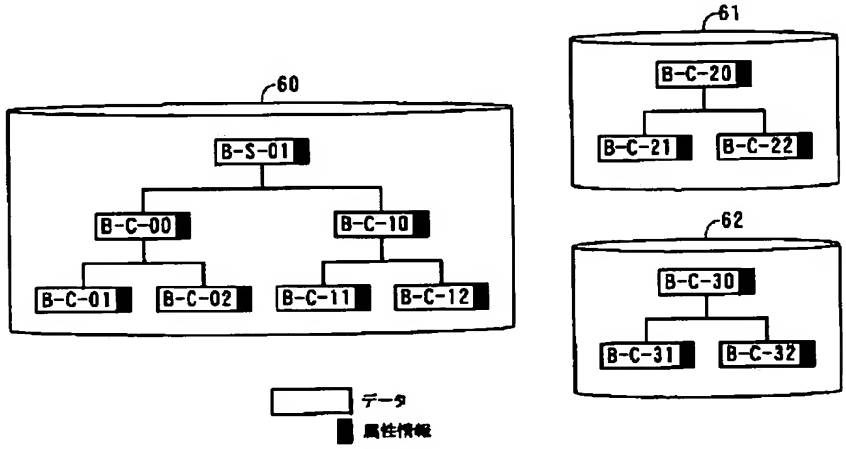
【図４】



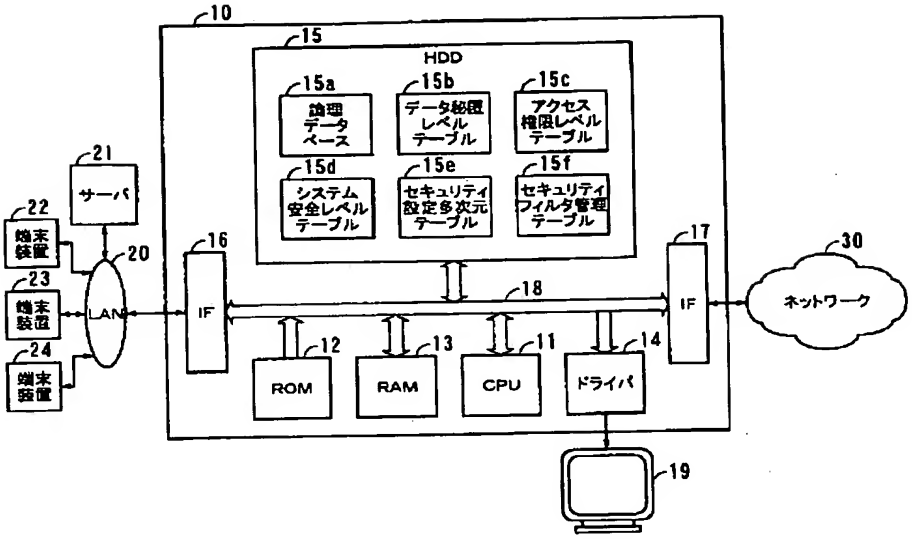
【図７】

資料名			秘匿レベル
PC	マザーボード	設計書	6
		コスト	10
		生産計画	5
	HDD	設計書	7
・	・	・	・
・	・	・	・
・	・	・	・

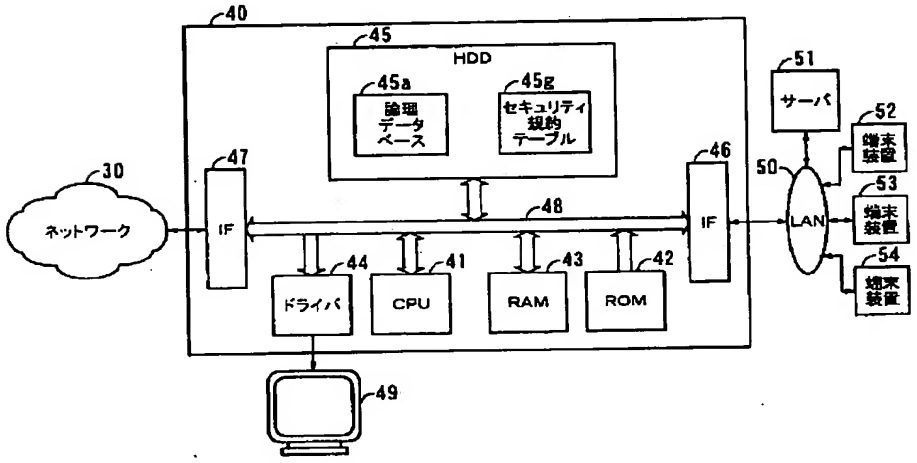
【図５】



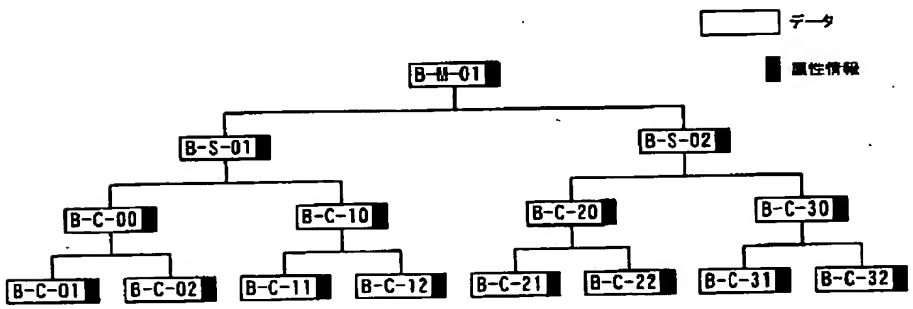
【図２】


10
15
HDD
15a
論理データベース
15b
データ秘匿レベルテーブル
15c
アクセス権限レベルテーブル
15d
システム安全レベルテーブル
15e
セキュリティ設定多次元テーブル
15f
セキュリティフィルタ管理テーブル
21
サーバ
22
端末装置
23
端末装置
24
端末装置
20
LAN
16
IF
18
17
IF
30
ネットワーク
12
ROM
13
RAM
11
CPU
14
ドライバ
19

【図３】


40
45
HDD
45a
論理データベース
45g
セキュリティ規約テーブル
51
サーバ
52
端末装置
53
端末装置
54
端末装置
30
ネットワーク
47
IF
48
46
IF
50
LAN
44
ドライバ
41
CPU
43
RAM
42
ROM
49

【図６】


データ
属性情報
B-M-01
B-S-01
B-S-02
B-C-00
B-C-10
B-C-20
B-C-30
B-C-01
B-C-02
B-C-11
B-C-12
B-C-21
B-C-22
B-C-31
B-C-32

【図８】

企業名	部門	ID	業務	アクセス権限レベル
F社	A部	01	PC	1
			HDD	3
	B部	01	ボード	1.5
G社	A部	01	HDD	2.1
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

【図９】

企業名	部門	ネット環境	システム環境	運用環境	総合環境
F社	A部	6	7	5	6
	B部	4	2	3	3
G社	A部	3	1	2.3	2.1
	B部	6	10	8	8
・	・	・	・	・	・
・	・	・	・	・	・
・	・	・	・	・	・

【図１０】

フィルタNo.	データ秘匿レベルα	アクセス権限レベルβ	システム安全レベルγ
1	$1 \leq \alpha < 5$	$2 < \beta \leq 6$	$2 < \gamma \leq 6$
2	$1 \leq \alpha < 5$	$2 < \beta \leq 6$	$6 < \gamma \leq 10$
3	$1 \leq \alpha < 5$	$6 < \beta \leq 10$	$2 < \gamma \leq 6$
4	$1 \leq \alpha < 5$	$6 < \beta \leq 10$	$6 < \gamma \leq 10$
5	$5 \leq \alpha < 9$	$2 < \beta \leq 6$	$2 < \gamma \leq 6$
6	$5 \leq \alpha < 9$	$2 < \beta \leq 6$	$6 < \gamma \leq 10$
7	$5 \leq \alpha < 9$	$6 < \beta \leq 10$	$2 < \gamma \leq 6$
8	$5 \leq \alpha < 9$	$6 < \beta \leq 10$	$6 < \gamma \leq 10$

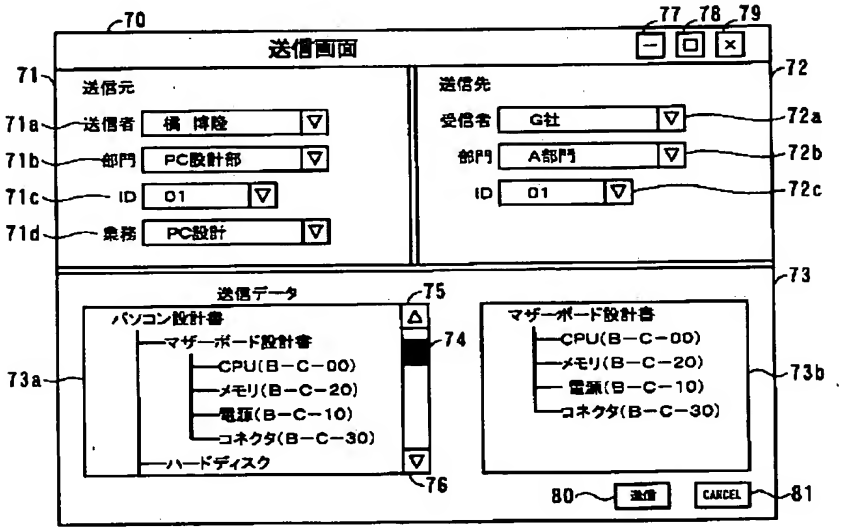
【図１１】

セキュリティ処理機能											
セキュリティフィルタNo.	a	b		c	d	e				f		…
	1	1	2	1	1	1	2	3	4	1	2	
1	①				②							
2	①											
3				①		②						
4					①	②						
5	①		②			③				④		
6	①		②				③				④	
7								①		②		
8									①		②	

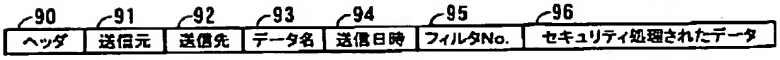
【図１２】

記号	分類	No.	処理内容
a	認証	1	PC−CARD
b	署名	1	PC−CARD
		2	MD5
c	電子すかし	1	W−MARK
d	ウィルス	1	VACCINE
e	圧縮	1	LHA
		2	COMPREBB
		3	GZIP
		4	FLDC
f	暗号	1	DES
		2	RSA
・	・	・	・
・	・	・	・
・	・	・	・

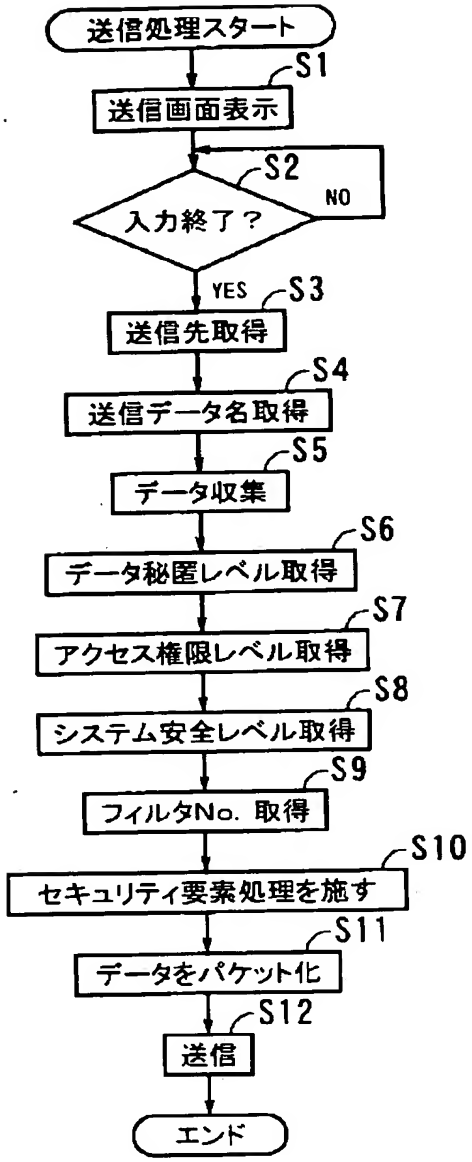
【図１４】



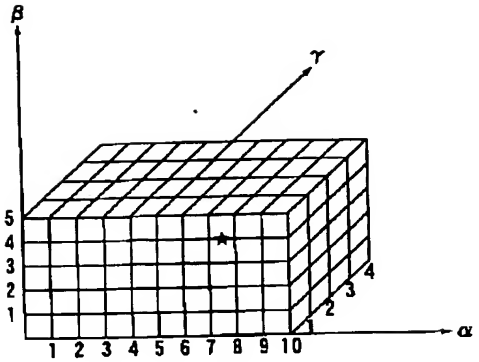
【図１８】



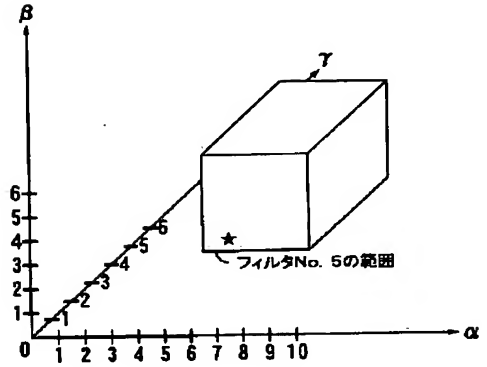
【図１３】



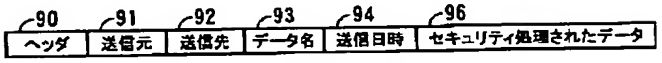
【図１５】



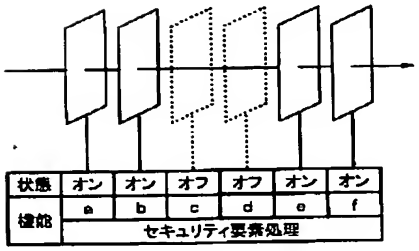
【図１６】



【図２９】



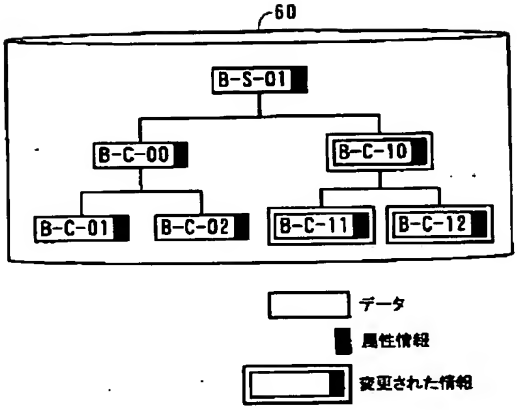
【図１７】



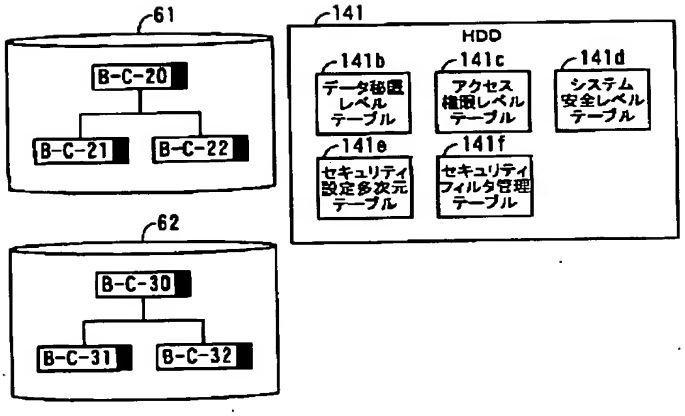
【図２１】

	資料名			秘匿レベル
PC	マザーボード	設計書	CPU	6
			電源	1
			メモリ	8
			コネクタ	6
		コスト		10
		生産計画		5
	HDD	設計書		7
⋮	⋮	⋮		⋮

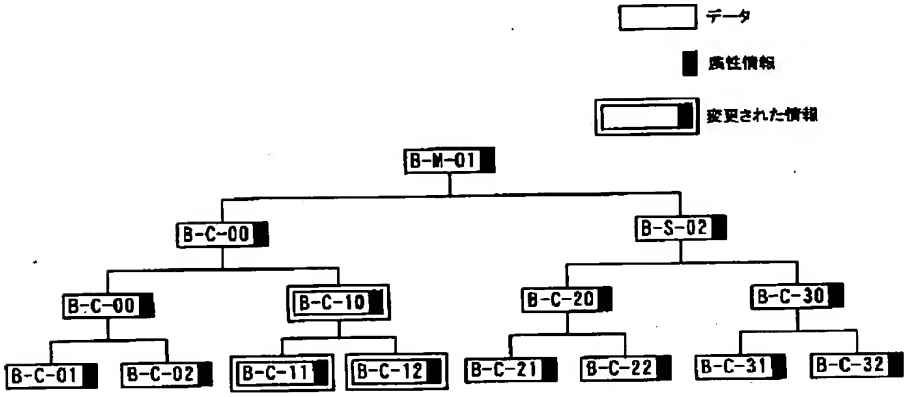
【図１９】



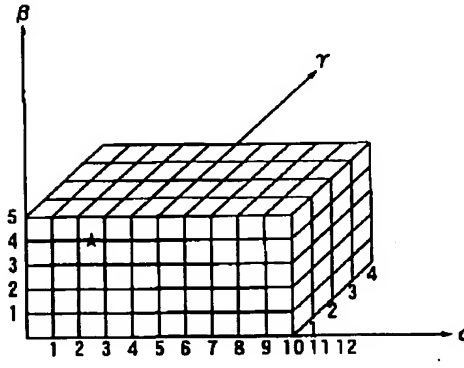
【図３２】



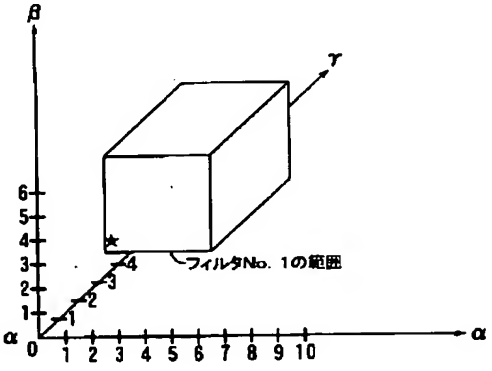
【図２０】



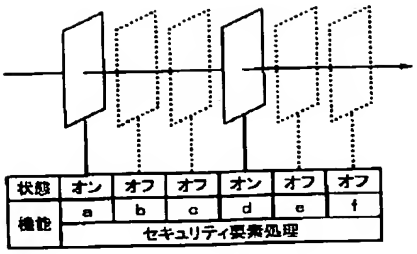
【図２２】



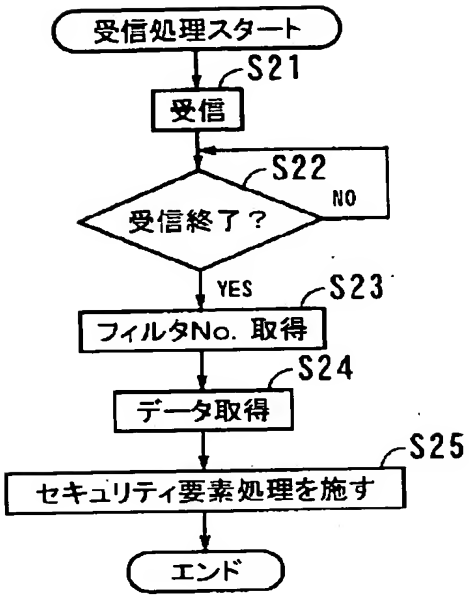
【図２３】



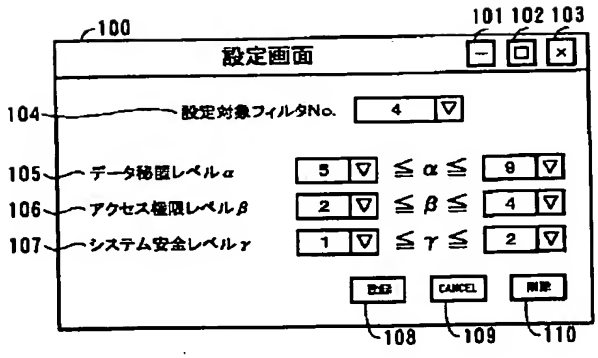
【図２４】


状態
オン
オフ
オフ
オン
オフ
オフ
機能
a
b
c
d
e
f
セキュリティ要素処理

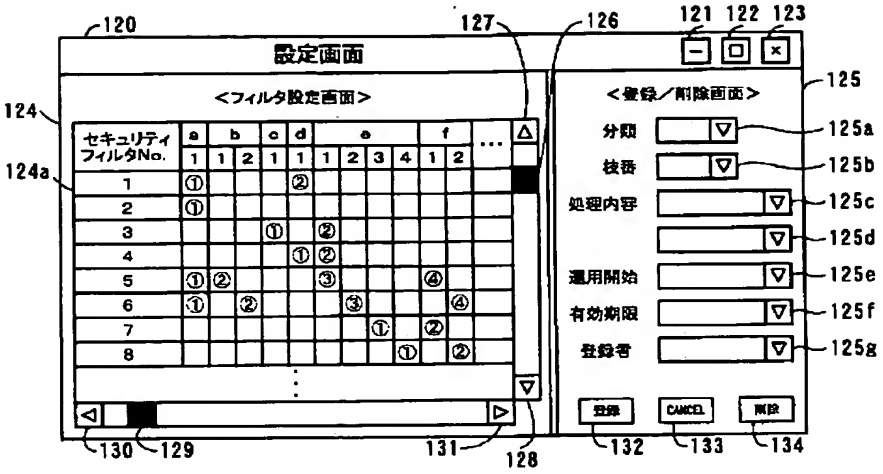
【図２５】


受信処理スタート
S21
受信
S22
NO
受信終了？
YES
S23
フィルタNo. 取得
S24
データ取得
S25
セキュリティ要素処理を施す
エンド

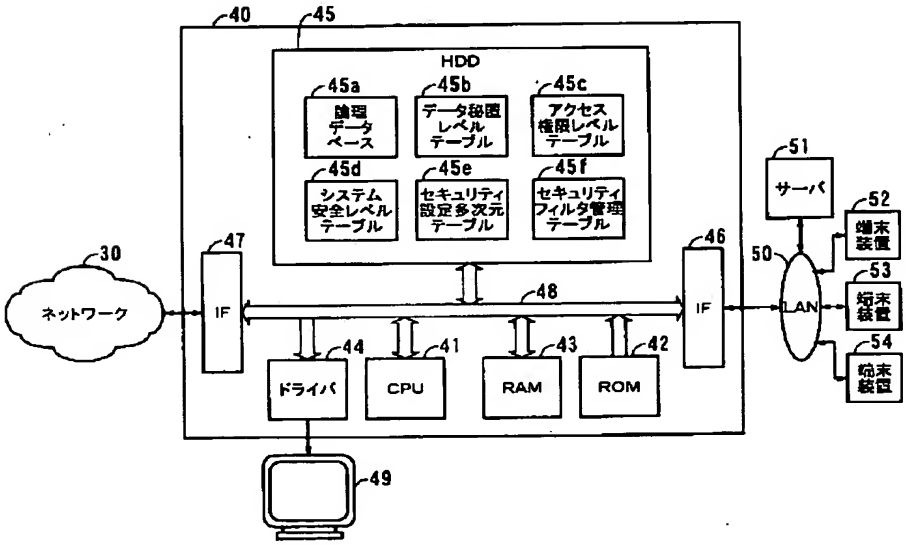
【図２６】


100
101 102 103
設定画面
104
設定対象フィルタNo.
4
105
データ秘匿レベルα
5
≦ α ≦
9
106
アクセス権限レベルβ
2
≦ β ≦
4
107
システム安全レベルγ
1
≦ γ ≦
2
CANCEL
108
109
110

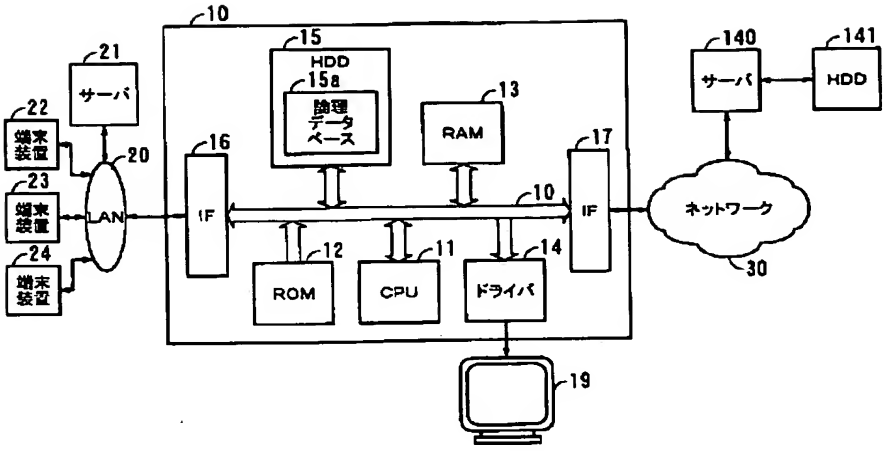
【図２７】


120
設定画面
127
126
121 122 123
125
<フィルタ設定画面>
<登録／削除画面>
124
124a
セキュリティフィルタNo.
a b c d e f
分類
125a
技番
125b
処理内容
125c
125d
運用開始
125e
有効期限
125f
登録者
125g
130 129 131 128
132 133 134

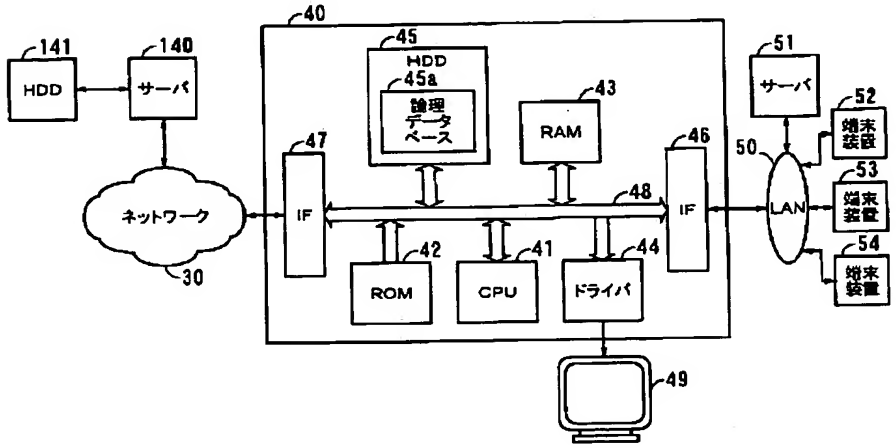
【図２８】


40
45
HDD
45a 論理データベース
45b データ秘匿レベルテーブル
45c アクセス権限レベルテーブル
45d システム安全レベルテーブル
45e セキュリティ設定多次元テーブル
45f セキュリティフィルタ管理テーブル
30
ネットワーク
47
IF
48
46
IF
50
LAN
51
サーバ
52
端末装置
53
端末装置
54
端末装置
44
ドライバ
41
CPU
43
RAM
42
ROM
49

【図３０】



【図３１】



【手続補正書】
【提出日】平成１１年１月１２日（１９９９．１．１２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項５
【補正方法】変更
【補正内容】
【請求項５】　前記送信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、受信側のアクセス権限レベルおよびシステム安全レベルを与える第１のテーブルと、得られたこれら３つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第２のテーブルとを更に有し、
前記セキュリティ処理手段は、前記第２のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、
前記特定情報付加手段は、セキュリティ処理が施されたデータに対して、施されたセキュリティ要素処理とその処理順序とを示す情報を特定情報として付加し、
前記特定情報抽出手段は、セキュリティ要素処理とその処理順序とを示す情報を受信したデータから抽出し、
前記セキュリティ処理解除手段は、抽出されたセキュリティ要素処理の組み合わせとその処理順序とを示す情報を参照して、セキュリティ処理を解除することを特徴とする請求項４記載のネットワークシステム。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項８
【補正方法】変更
【補正内容】
【請求項８】　前記送信装置および受信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、受信側のアクセス権限レベルおよびシステム安全レベルを与える第１のテーブルと、得られたこれら３つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第２のテーブルとを更に有し、
前記セキュリティ処理手段は、前記第２のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、
前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、
前記特定情報抽出手段は、受信したデータから前記送信元名とデータ名とを抽出し、
前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせと処理順序を前記第１および第２のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項４記載のネットワークシステム。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】請求項９
【補正方法】変更
【補正内容】
【請求項９】　前記送信装置および受信装置の双方がアクセスできるネットワーク上の所定の位置に、送信しようとするデータのデータ秘匿レベル、ならびに、受信側のアクセス権限レベルおよびシステム安全レベルを与える第１のテーブルと、得られたこれら３つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第２のテーブルとを更に有し、
前記セキュリティ処理手段は、前記第２のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、
前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、
前記特定情報抽出手段は、前記送信元名とデータ名とを受信したデータから抽出し、
前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせとその処理順序とを前記第１および第２のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項４記載のネットワークシステム。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】変更
【補正内容】
【００２６】送信手段１ｆは、特定情報が付加されたデータをネットワーク４を介して受信装置５に向けて送信する。受信装置５の受信手段５ａは、ネットワーク４を介して送信装置１から伝送されてきたデータを受信し、特定情報抽出手段５ｂに供給する。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００６１
【補正方法】変更
【補正内容】
【００６１】例えば、データ秘匿レベルαが範囲（$1 \leqq \alpha < 5$）内にあり、アクセス権限レベルβが範囲（$2 < \gamma \leqq 6$）内にあり、また、システム安全レベルが範囲（$2 < \beta \leqq 6$）内にある場合には、表の第１番目の項目であるＮｏ．１のフィルタが選択されることになる。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００７２
【補正方法】変更
【補正内容】
【００７２】リストボックス７３ａにおいて送信対象となるデータを選択すると、選択された内容は送信されるデータとしてエディットボックス７３ｂに表示される。
［Ｓ２］ＣＰＵ１１は、図１４に示す送信画面において全ての必要項目の入力が終了し、送信ボタン８０が操作された場合にはステップＳ３に進み、それ以外の場合にはステップＳ２に戻る。
［Ｓ３］ＣＰＵ１１は、図１４に示す送信画面において入力された送信先に関する情報を取得する。

フロントページの続き

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　林　武彦
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B085 AE06 AE23 AE29
5K013 AA02 BA02 EA01 FA03 GA05